UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,814	03/14/2005	Jarmo Talvitie	3502-1075	4622

466 7590 01/05/2007

YOUNG & THOMPSON
745 SOUTH 23RD STREET
2ND FLOOR
ARLINGTON, VA 22202

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/527,814	TALVITIE, JARMO	
	Examiner	Art Unit	
	Jenise E. Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/14/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claim 38 is objected to because of the following informalities: Claim 38 ends with the word, "viru". The Examiner assumes the Applicant means viruses. The claim has been rejected as such. Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-38 are rejected under 35 U.S.C. 102(e) as being anticipated by Chefalas et al(2002/0116639).

4. As per claim 1, Chefalas et al. discloses a security system for repelling viruses in computers and computer networks[0012], which security system is adapted to forward messages[0012, 0030], characterized in that the security system includes a first sub-system to detect unknown viruses, which sub-system is adapted in connection with the forwarding of messages or with other action or, in a timed manner, to perform at least one action to activate unknown viruses[0012, 0028, 0030].

5. As per claim 2, Chefalas et al. discloses characterized in that it is adapted to forward an

alarm caused by the detection of a virus to at least one system connected to the security system[0012].

6. As per claim 3, Chefalas et al. discloses characterized in that it is adapted to break the connection to at least one other system on the basis of an alarm caused by the detection of a virus[0030, 0046].

7. As per claim 4, Chefalas et al. discloses characterized in that it additionally includes a second sub-system for forwarding messages from the first sub-system to at least one system connected to the security system[0012, 0054].

8. As per claim 5, Chefalas et al. discloses characterized in that it additionally includes a third sub-system that is adapted to break the connection to at least one other sub-system upon receiving an alarm[0030].

9. As per claim 6, Chefalas et al. discloses characterized in that the second sub-system includes an identifier, which corresponds identifier of the apparatus of the third sub-system[0044-0045, 0047].

10. As per claim 7, Chefalas et al. discloses a security system, characterized in that the first sub-system is adapted to monitor its actions to detect viruses[0012].

11. As per claim 8, Chefalas et al. discloses characterized in that the alarm is a message or at least a part of a message that is forwarded to the recipient quicker than other communications[0012, 0028].

12. As per claim 9, Chefalas et al. discloses characterized in that the third sub-system includes at least one computer or one network element including a computer[0030].

13. As per claim 10, Chefalas et al. discloses characterized in that the alarm is forwarded via

a separate connection[0012].

14. As per claim 11, Chefalas et al. discloses characterized in that the said action is handling of files[0044].

15. As per claim 12, Chefalas et al. discloses a security system characterized in that it is adapted to detect an activated virus: a change takes place in the first sub-system prior to actions causing changes carried out by the first-mentioned sub-system, a change takes place in the first sub-system[0012].

16. As per claims 13, 27, 35, Chefalas et al. discloses characterized in that it is adapted to combine activation measures of viruses to take place consecutively in time[0046].

17. As per claims 14, 28, 36, Chefalas et al. discloses characterized in that it is adapted to logics when trying to activate viruses: pre-programmed [0060].

18. As per claim 15, Chefalas et al. discloses a security system, characterized in that to it has been connected parallel with a third sub-system a system that is adapted to save a message sent from the third sub-system[0030].

19. As per claim 16, Chefalas et al. discloses characterized in that the first sub-system is adapted to compare in a parallel system a message sent from the third sub-system to the first sub-system and additionally saved in the parallel system in order to detect an anomaly caused by a virus[0054].

20. As per claim 17, Chefalas et al. discloses characterized in that the above-mentioned parallel system is adapted to forward a message saved by it[0012].

21. As per claim 18, Chefalas et al. discloses characterized in that it is adapted to examine messages forwarded through it in order to detect known viruses[0012, 0054].

22. As per claim 19, Chefalas et al. discloses characterized in that in order to isolate data between the first and the second system, it has been adapted to transfer data between the first and the second system through the first and the second sub-system[0012], which security system is adapted to disrupt the connection between the first system, and the first sub-system before a connection is established between the first and the second sub-system, and is adapted to disrupt the connection between the first and the second sub-system before a connection is established between the second sub-system and the second system[0054] .

23. As per claim 20, Chefalas et al. discloses a security system for repelling viruses in computers and computer networks, which security system is adapted to forward messages, characterized in that the security system includes a first sub-system for detecting unknown viruses[0012], which first sub-system is adapted to compare messages with at least partially identical identifiers with each other in order to detect unknown viruses[0044-0045, 0047, 0058].

24. As per claim 21, Chefalas et al. discloses a security system, characterized in that it is adapted to request the sender of the above-mentioned messages with the same identifiers to re-send at least one message with the same identifier and further adapted to compare at least one re-sent message received with the above-mentioned original messages in order to detect messages containing viruses[0044-0045, 0047, 0058].

25. As per claim 22, Chefalas et al. discloses a method for repelling viruses in computers and data networks, characterized in that it is carried out in a security system including a first sub-system for forwarding messages and for detecting viruses[0012], which first sub-system can, with regard to data transfer, be isolated from the rest of the system[0028], which method includes the steps where: the functions of the system are monitored in order to detect a

virus[0028], a virus is detected when: a change takes place in the first sub-system prior to actions causing changes carried out by the first-mentioned sub-system[0028, 0030].

26. As per claim 23, Chefalas et al. discloses a method for repelling viruses in computers and computer networks, characterized in that the method has stages where: at least one action in the system is taken in connection with the forwarding of messages or other action, or in a timed manner, in order to activate a virus, the actions of the system are monitored in order to detect an occurrence initiated by virus activation, an alarm is given when a virus is detected[0012, 0028].

27. As per claim 24, Chefalas et al. discloses characterized in that the system running it includes a first sub-system for forwarding of messages and for detecting of viruses, which first sub-system can be isolated from another system as to communications[0028].

28. As per claims 25, 32, Chefalas et al. discloses characterized in that the action taken to activate a virus is handling of files[0050, 0060]

29. As per claim 26, Chefalas et al. discloses a characterized in that it is run in a security system including a first sub-system and a second sub-system in which method the activation of a virus is detected when at least one of the following conditions is met: a change takes place in the first sub-system prior to actions causing changes carried out by the first-mentioned sub-system, a change takes place in the first sub-system[0012]

30. As per claim 29, Chefalas et al. discloses characterized in that it also includes a stage where known viruses are searched for on the basis of their characteristics[0032].

31. As per claim 30, Chefalas et al. discloses characterized in that in order to isolate data between the first and the second system the method is run in a security system that includes a first and a second sub-system through which sub-systems data is transferred between the first and

the second system phase by phase[0012], in which phases: the connection for data transfer is disrupted between the first system and the first sub-system, a connection for data transfer is established between the first sub-system and the second sub-system, the connection for data transfer is disrupted between the first sub-system and the second sub-system, a connection for data transfer is established between the second sub-system and the second system[0054].

32. As per claim 31, Chefalas discloses an apparatus for repelling viruses in computers and computer networks, which apparatus includes equipment for saving data and for handling data and equipment for transferring data with another apparatus, characterized in that the apparatus is adapted to receive a message from the said other apparatus and to perform at least one action to activate viruses contained in the message[0028, 0030].

33. As per claim 33, Chefalas discloses characterized in that it is adapted to detect virus activation when at least one of the following conditions is met: a change takes place prior to actions caused by changes made by the apparatus[0012].

34. As per claim 34, Chefalas discloses characterized in that it is adapted to send a message, and it is adapted to detect virus activation when: a message leaves without authorization from the anti-virus software of the apparatus[0030, 0032].

35. As per claim 37, Chefalas discloses characterized in that it is adapted to examine the message mentioned in order to detect known viruses[0032].

36. As per claim 38, Chefalas discloses characterized in that it is adapted to monitor its functions in order to detect viruses[0012, 0030].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E. Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 16, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER